DOD PRIVACY IMPACT ASSESSMENT (PIA)

1. Department of Defense Component

Assistant Chief of Staff for Installation Management (ACSIM), Family & Morale, Welfare and Recreation Command

2. Name of Information Technology (IT) System (APMS System Name)

Eventmaster

3. Budget System Identification Number (SNAP-IT Initiative Number).

9990

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).

2976

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable).

N/A

6. Privacy Act System of Records Notice Identifier (if applicable).

A0215 CFSC, General Morale, Welfare, Recreation and Entertainment Records
(October 17, 2001, 66 FR 52750)

The system notice will be updated specific to this data collection.

7. OMB Information Collection Requirement Number (if applicable) and expiration date.

N/A

8. Type of authority to collect information (statutory or otherwise).

10 U.S.C. 3013, Secretary of the Army;
26 U.S.C. 6041, Information at Source;
Army Regulation 215-1, Morale, Welfare and Recreations Activities and Non-appropriated Fund Instrumentalities;
Army Regulation 215-3, Nonappropriated Fund Personnel Policy;
Army Regulation 215-4, Nonappropriated Fund Contracting;
Army Regulation, 608-10 Child Development Services;

DoD Directive 1015.2, Military Morale, Welfare and Recreation (MWR);
DoD Instruction 1015.10, Program for Military Morale, Welfare and Recreation (MWR);
E.O. 9397 (SSN)

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries, and interconnections, location of system and components, and system backup).

EventMaster is a component of the U.S. Army MWR MIS AIS. The purpose of the EventMaster application is to provide the tools needed to expedite the catering process. The EventMaster software contains the following feature: Bookings, Pre-event costing, proposal letters and graphic display of event function rooms. The software allows the caterer to maximize room, maximize sales potential, facilitate immediate changes, ensure accuracy in ordering and production and numerous management reports. EventMaster is currently in the sustainment phase of the life cycle process. The MWR MIS AIS is a mission essential system that provides the Executive Control and Essential Command Supervision (ECECS) for the Garrison Commander, IMCOM, ACSIM and FMWRC functional proponents. Communications with the MWR MIS AIS is TCP/IP 10/100 including: direct connection using DOIM infrastructure, or paired DSL modems over the existing post telephone infrastructure. The system owner is Deputy CIO, USA FMWRC-IM-MIS. The MWR MIS AIS forms the central point for network services and database control for the MWR MIS network. This "sub" network connects to the base network over a connection that is provided by, and is the responsibility of, the installation DOIM. Connections between remote terminals and the MWR MIS AIS can made directly, over DOIM provided links, or entire facilities can be linked to the base network and routed back to the MWR MIS AIS. All systems that connect to the MWR MIS AIS must use a Novell authentication

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.).

Name, address, information from official government ID cards (SSN, date of birth, sponsor), phone number, email, fax number, payment type (check, credit card, lending institution, routing and account numbers) customer type (active military or civilian, alumni group, retiree, dependent). The customer is the source.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

The information is collected from the customer verbally and then entered manually into the system by employees of the facility.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a DA program, etc.)

The information is collected in order to allow individuals to reserve and use facilities for recreational and official business purposes.

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).

The information is used to establish a party contract, and to establish the responsible patron for the party contract and requisite billing invoices.

14. Describe whether the system derives or creates new data about individuals through aggregation.

This system does not create new data about individuals through aggregation

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

Data is shared with activity clerks, chef, caterers, accounting, managers and MWR system administrator. Access to data is restricted based on need to know. Information is available to authorized users in order to perform official government duties. For example, chefs view menu information, date and time of the event, but they do not have access to accounting information. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

Contacting MWR to reserve a facility is taken as an indication of willingness to provide PII. Individuals who do so are provided the appropriate Privacy Act advisory statement. In order to complete the contract the customer must sign validating that the information provided is correct and applicable.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

The customer is provided a Privacy Act Statement or one is explained during the initial contact interview. A contract is produced by the system and provided to the individual for review and signature. A copy is given to the customer.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

Access to the data is controlled by username and password authentication and further narrowed by role. For example, chefs can view menu information, date and time of the event but they do not have access to accounting. Data access is controlled by rights granted/restricted according to user type, user ID and password. Novell authentication restricts access to the data by personnel who do not have a need to know. The Novell authentication assures the requisite Confidentiality and Integrity of the data. Local connections to the Installation LAN are provided by DOIM where applicable. Backup of system and data files are accomplished weekly, and incremental backups of data files are done daily. These backups are conducted according to instructions provided in the NetWare product documentation. Both full and incremental backup media are stored securely off-site in fireproof containers. Local copies of backup data are held provided they are similarly secured and protected. Copies of all applications and current patches are kept updated and stored offsite in fireproof containers.

This system has a current certification and accreditation. The system resides on secure military installations within secured facilities.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

A systems notice currently exists. Either the current notice will be amended to be more descriptive of this business practice, or an entirely new system notice will be developed.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There is no risk in providing individual the opportunity to object or consent,

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

The data in the system is For Official Use Only. The PIA may be published in full.